## CLAIMS

What is claimed is:

1. A method for automatically generating network address translation (NAT) data to enable a private host having a private IP address to communicate with a public host having a first public IP address, said private host being connected to a private network, said public host being connected to a public network, comprising:

providing automated NAT provision software, said software, responsive to communication initiated by one of said private host and said public host, consulting a security policy associated with said private host to determine whether said communication between said private host and said public host is permissible; and

if said consulting indicates that said communication between said private host and said public host is permissible, provisioning automatically using said software and without a human operator intervention after said consulting, in a database a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

2. The method of claim 1 wherein said security policy is implemented using an access list.

3. The method of claim 2 wherein said second public IP address represents a shared public IP address if said communication is initiated by said private host.

4. The method of claim 2 wherein said second public IP address represents a dedicated public IP address if said communication is initiated by said public host.

5. The method of claim 1 wherein said database represents a Network Address Translation (NAT) table.

6. The method of claim 1 further including:

detecting a removal of said private host from said private network; and

removing, using said software, said second public IP address from said database responsive to said detecting said removal of said private host.

7. The method of claim 1 wherein said security policy represents a generic security policy.

8. The method of claim 7 further comprising automatically generating NAT data for all private hosts affected by said generic policy after said generic policy is modified using said software.

9. An article of manufacture comprising a program storage medium having computer readable code embodied therein, said computer readable code being configured to automatically generate network address translation (NAT) data to enable a private host having a private IP address to communicate with a public host having a first public IP address, said private host being connected to a private network, said public host being connected to a public network, comprising:

computer readable code for providing automated NAT provision software, said software consulting a security policy associated with said private host to determine whether communication between said private host and said public host is permissible; and

computer readable code for provisioning, in a database using said software, if said consulting indicates that said communication between said private host and said public host is permissible, a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

10. The article of manufacture of claim 9 wherein said security policy is implemented using an access list.

11. The article of manufacture of claim 10 wherein said second public IP address represents a shared public IP address if said communication is initiated by said private host.

12. The article of manufacture of claim 10 wherein said second public IP address represents a dedicated public IP address if said communication is initiated by said public host.

13. The article of manufacture of claim 9 wherein said database represents a Network Address Translation (NAT) table.

14. The article of manufacture of claim 9 further including:

computer readable code for detecting a removal of said private host from said private network; and

computer readable code for removing, using said software, said second public IP address from said database responsive to said detecting said removal of said private host.

15. The article of manufacture of claim 9 wherein said security policy represents a generic security policy.

16. The article of manufacture of claim 15 further comprising computer readable code for automatically generating NAT data for all private hosts affected by said generic policy after said generic policy is modified using said software.

17. A method for automatically generating network address translation (NAT) data in a NAT table to enable communication between a private host having a private IP address and a public host having a first public IP address, said private host being connected to a private network, said public host being connected to a public network, comprising:

consulting, using automated NAT provision software, a security policy associated with said private host to determine whether said communication between said private host and said public host is permissible, said consulting being performed responsive to a message initiated by one of said private host and said public host; and

if said consulting indicates that said communication between said private host and said public host is permissible, provisioning automatically using said software and without a human operator intervention after said consulting, in said NAT table a second public IP address for address translation between said private IP address and said second public IP address, said second public IP address being employed as one of a source IP address and a destination IP address for routing said communication between said private host and said public host through said public network.

18. The method of claim 17 wherein said second public IP address represents a shared public IP address if said communication is initiated by said private host.

19. The method of claim 17 wherein said second public IP address represents a dedicated public IP address if said communication is initiated by said public host.